

Quantum Measurements for Hidden Subgroup Problems with Optimal Sample Complexity

Masahito Hayashi*
masahito@qci.jst.go.jp

Akinori Kawachi†
kawachi@is.titech.ac.jp

Hirotsada Kobayashi‡
hirotada@nii.ac.jp

*ERATO-SORST Quantum Computation and Information Project
Japan Science and Technology Agency
5-28-3 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan

†Department of Mathematical and Computing Sciences
Tokyo Institute of Technology
2-12-1 Ookayama, Meguro-ku, Tokyo 152-8552, Japan

‡Principles of Informatics Research Division
National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan

Abstract

One of the central issues in the hidden subgroup problem is to bound the sample complexity, i.e., the number of identical samples of coset states sufficient and necessary to solve the problem. In this paper, we present general bounds for the sample complexity of the identification and decision versions of the hidden subgroup problem. As a consequence of the bounds, we show that the sample complexity for both of the decision and identification versions is $\Theta(\log |\mathcal{H}| / \log p)$ for a candidate set \mathcal{H} of hidden subgroups in the case that the candidate subgroups have the same prime order p , which implies that the decision version is at least as hard as the identification version in this case. In particular, it does so for the important instances such as the dihedral and the symmetric hidden subgroup problems. Moreover, the upper bound of the identification is attained by the pretty good measurement. This shows that the pretty good measurement can identify any hidden subgroup of an arbitrary group with at most $O(\log |\mathcal{H}|)$ samples.

1 Introduction

1.1 Background

The *hidden subgroup problem* is one of the central issues in quantum computation, which was introduced for revealing the structure behind exponential speedups in quantum computation [34].

Definition 1.1 (Hidden Subgroup Problem (HSP)) Let G be a finite group. For a hidden subgroup $H \leq G$, we define a map f_H from G to a finite set S with the property that $f_H(g) = f_H(gh)$ if and only if $h \in H$. Given $f_H : G \rightarrow S$ and a generator set of G , the hidden subgroup problem (HSP) is the problem of finding a set of generators for the hidden subgroup H . We say that HSP over G is efficiently solvable if we can construct an algorithm in time polynomial in $\log |G|$.

The nature of many existing quantum algorithms relies on efficient solutions to Abelian HSPs (i.e., HSPs over Abelian groups) [41, 28, 5, 6]. In particular, Shor's celebrated quantum algorithms for factoring and discrete logarithm essentially consist of reductions to certain Abelian HSPs and efficient solutions to the Abelian HSPs [40]. Besides his results, many efficient quantum algorithms for important number-theoretic problems (e.g., Pell's equation [15] and unit group of a number field [16, 38]) were based on solutions to Abelian HSPs.

Recently, non-Abelian HSPs have also received much attention. It is well known that the graph isomorphism problem can be reduced to the HSP over the symmetric group [5, 3] (more strictly, the HSP over $S_n \wr S_2$ [8]). Regev showed that we can construct an efficient quantum algorithm for the unique shortest vector problem if we find an efficient solution to HSP over the dihedral group under certain conditions [36]. While the efficient quantum algorithm for general Abelian HSPs has been already given [28, 34], the non-Abelian HSPs are extremely harder than the Abelian ones. There actually exist efficient quantum algorithms for HSPs over several special classes of non-Abelian groups [37, 11, 18, 12, 14, 23, 24, 30, 2]. Nonetheless, most of important cases of non-Abelian HSPs, including the dihedral and symmetric HSPs, are not known to have efficient solutions. Thus, finding efficient algorithms for non-Abelian HSPs is one of the most challenging issues in quantum computation.

The main approach to the non-Abelian HSPs is based on a generic framework called the *standard method*. To our best knowledge, all the existing quantum algorithms for HSPs essentially contain this framework. The standard method essentially reduces HSPs to the quantum state identification [39] for the so-called *coset states*, which contain information of the hidden subgroup.

Definition 1.2 (Coset State and Standard Method) Let G be any finite group and H be the hidden subgroup of G . We then define the *coset state* ρ_H for H as $\rho_H = \frac{1}{|G|} \sum_{g \in G} |gH\rangle\langle gH| = \frac{|H|}{|G|} \sum_{g \in G/H} |gH\rangle\langle gH|$, where $|gH\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |gh\rangle$.

Standard Method with k Coset States

- (1) Prepare two registers with a uniform superposition over G in the first register and all zeros in the second register: $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|0\rangle$.
- (2) Compute $f_H(g)$ and store the result to the second register: $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|f_H(g)\rangle$.
- (3) Discard the second register to obtain a coset state: $\rho_H = \frac{|H|}{|G|} \sum_{g \in G/H} |gH\rangle\langle gH|$.
- (4) Repeat (1)–(3) k times and then apply a quantum measurement to k samples of ρ_H .

Thus the main task for solving HSP based on the standard method is to find an efficiently implementable quantum measurement extracting the information of the hidden subgroup from identical samples of the coset state.

Many researchers have broadly studied hard instances of non-Abelian HSPs from positive and negative aspects based on the standard method. In particular, they have focused on the *sample complexity* of HSPs, i.e., how many coset states are sufficient and necessary to identify the hidden subgroup with a constant success probability.

In several classes of the non-Abelian HSPs for which efficient algorithms are unknown, it is shown that we can identify any hidden subgroup by (possibly inefficient) classical post-processes using the classical information obtained by the quantum Fourier transforms to polynomially many samples of coset states [9, 18, 14, 30].

Bacon, Childs and van Dam demonstrated that the so-called *pretty good measurement* (PGM, also known as the *squire root measurement* or *least squares measurement* [20]) is optimal for identifying coset states in view of the sample complexity on a class of semidirect product groups $A \rtimes \mathbb{Z}_p$ including the dihedral group, where A is any Abelian group and p is a prime [2]. They proved that the sample complexity is $\Theta(\log |A| / \log p)$ to identify the hidden subgroup by the PGM from the candidate set $\mathcal{H}_{\text{SDP}} = \{ \langle (a, 1) \rangle < A \rtimes \mathbb{Z}_p : a \in A \}$. Moore and Russell generalized their result to prove the optimality of the PGM for a wider class of HSPs [31]. They actually gave the PGM for identifying coset states of hidden conjugates of a subgroup, i.e., hidden subgroups having form of $g^{-1}Hg$ for a fixed non-normal subgroup H of a finite group G and $g \in G$. These results of [2, 31] showed that the PGM succeeds for a wide class of HSPs with at most $O(\log |\mathcal{H}|)$ samples for the candidate set \mathcal{H} of hidden subgroups. For a more general case, Ettinger, Høyer and Knill gave a bounded-error quantum measurement that solves HSP over any finite group G with $O(\log^2 |G|)$ samples of coset states (Theorem 2 in [10]). They also constructed an error-free measurement for the general HSP with the same sample complexity $O(\log^2 |G|)$ within a constant factor in [10] by combining the bounded-error one with the amplitude amplification technique [7].

These quantum measurements ignore the time complexity issue in general. However, they may lead to efficient quantum algorithms for HSPs. Bacon et al. actually gave efficient implementation of the PGM for identifying given coset states on a class of the semidirect groups including the Heisenberg group [2], i.e., they

constructed an efficient quantum algorithm for the HSPs from the corresponding PGMs. Hence, to give the quantum measurements for identification of given coset states like PGMs may play important roles towards the construction of efficient quantum algorithms for HSPs.

The negative results of the standard method has also been studied from an information-theoretic viewpoint, which are based on a decision version of the HSP defined as the problem of deciding whether the hidden subgroup is trivial or not. In particular, the difficulty of the HSP over the symmetric group S_n has been shown by a number of results for this decision version [18, 14, 27, 33, 32]. Hallgren et al. recently proved that a joint measurement across multiple samples of coset states is essentially required to solve a decision version over the symmetric group, which is deeply related to the graph isomorphism problem. More precisely, they showed that joint quantum measurements across $\Omega(n \log n)$ samples of coset states are necessary to decide whether the given samples are generated from the trivial subgroup $\{id\}$ or a subgroup in $\mathcal{H}_{\text{Sym}} = \{H < S_n : H = \langle h \rangle, h^2 = id, h(i) \neq i (i = 1, \dots, n)\}$, i.e., a set of all the subgroups generated by the involution composed of $n/2$ disjoint transpositions [17].

1.2 Our Contributions

We study upper and lower bounds for the sample complexity of general HSPs from an information-theoretic viewpoint. We consider two problems associated with HSPs to deal with their sample complexity. The first one is the identification version for solving HSPs based on the standard method.

Definition 1.3 (Coset State Identification (CSI)) Let \mathcal{H} be a set of candidate subgroups of a finite group G . We then define $S_{\mathcal{H}}$ as a set of coset states corresponding to \mathcal{H} . Given a black box that generates an unknown coset state ρ_H in $S_{\mathcal{H}}$, the Coset State Identification (CSI) for \mathcal{H} is the problem of identifying $H \in \mathcal{H}$.

One can easily see that any solution to HSP based on the standard method reduces this identification of coset states. We now define the sample complexity of CSI for \mathcal{H} as the sufficient and necessary number of samples for identifying the given coset state with a constant probability.

The second one is the decision version, named the Triviality of Coset State. Special cases of this problem have been discussed for the limitations of the standard method in many previous results [18, 14, 27, 32, 33, 1, 17].

Definition 1.4 (Triviality of Coset State (TCS)) Let \mathcal{H} be a set of candidate non-trivial subgroups of a finite group G , i.e., $H \neq \{id\}$ for every $H \in \mathcal{H}$. We then define $S_{\mathcal{H}}$ as a set of coset states corresponding to \mathcal{H} . Given a black box that generates an unknown state σ that is either in $S_{\mathcal{H}}$ (i.e., a coset state for the non-trivial subgroup) or equal to $I/|G|$ (i.e., a coset state for the trivial subgroup), the Triviality of Coset State for $S_{\mathcal{H}}$ is the problem of deciding whether σ is in $S_{\mathcal{H}}$ or equal to $I/|G|$. We say that a quantum algorithm solves TCS with a constant advantage if it correctly decides whether a given state is in $S_{\mathcal{H}}$ or equal to $I/|G|$ with success probability at least $1/2 + \delta$ for some constant $\delta \in (0, 1/2]$.

Similarly to the case of CSI, we define the sample complexity of TCS for \mathcal{H} as the sufficient and necessary number of coset states to solve TCS with a constant advantage.

Note that this problem might be efficiently solvable even if we cannot identify the hidden subgroup. Actually, if we can give a solution to TCS for $\mathcal{H}_{\text{Sym}} = \{H < S_n : H = \langle h \rangle, h^2 = id, h(i) \neq i (i = 1, \dots, n)\}$, we can also solve the rigid graph isomorphism problem, i.e., the problem of finding an isomorphism between two graphs having no non-trivial automorphisms, and the decisional graph automorphism problem, i.e., the problem of deciding whether a given graph has non-trivial automorphisms or not [29].

In this paper, we give bounds of the sample complexity of CSI and TCS by simple information-theoretic arguments. We present the following bounds of the sample complexity of CSI.

Theorem 1.5 (Upper and Lower Bounds for CSI) Let \mathcal{H} be any set of candidate subgroups of a finite group. Then, the sample complexity of CSI for \mathcal{H} is at most $O\left(\frac{\log |\mathcal{H}|}{\log \min_{H \neq H' \in \mathcal{H}} (|H|/|H \cap H'|)}\right)$ and at least $\Omega\left(\frac{\log |\mathcal{H}|}{\log \max_{H \in \mathcal{H}} |H|}\right)$.

Moreover, the upper bound of CSI can be attained by the PGM. This shows that we can identify a hidden subgroup for an arbitrary group G by the PGM with at most $O(\log |\mathcal{H}|)$ samples, which is a wider class than those of the previous results [2, 31]. It is noted that the essentially same upper bound* for CSI follows from the result of Ettinger et al. [10]. However, their measurement is not known to be a pretty good measurement.

We also present the following bounds of the sample complexity of TCS.

Theorem 1.6 (Upper and Lower Bounds for TCS) Let \mathcal{H} be any set of candidate subgroups of a finite group. Then, the sample complexity of TCS for \mathcal{H} is at most $O\left(\frac{\log |\mathcal{H}|}{\log \min_{H \in \mathcal{H}} |H|}\right)$. If $|H|$ is a prime for every $H \in \mathcal{H}$, the sample complexity is at least $\Omega\left(\frac{\log |\mathcal{H}|}{\log \max_{H \in \mathcal{H}} |H|}\right)$.

Summarizing these bounds, we obtain the following tight bounds for a class of CSI and TCS including several important instances such as \mathcal{H}_{SDP} and \mathcal{H}_{Sym} .

Corollary 1.7 Let \mathcal{H} be any set of candidate subgroups of a finite group satisfying that $|H| = p$ for every $H \in \mathcal{H}$, where p is a prime. Then, the sample complexity of CSI and TCS for \mathcal{H} is $\Theta\left(\frac{\log |\mathcal{H}|}{\log p}\right)$.

This theorem implies that the decision version is as hard as the corresponding identification version in view of the sample complexity for this class.

We moreover apply our arguments to evaluation of information-theoretic security of the quantum encryption schemes proposed by Kawachi et al. [25, 26]. They proposed two quantum encryption schemes: One is a single-bit encryption scheme, which has a computational security proof based on the worst-case hardness of the decisional graph automorphism problem, and the other is a multi-bit encryption scheme, which has no security proof. Since their schemes make use of quantum states quite similar to coset states over the symmetric group as the encryption keys and ciphertexts, our proof techniques are applicable to the security evaluation of their schemes. We prove that the success probability of any computationally unbounded adversary distinguishing between any two ciphertexts is at most $\frac{1}{2} + 2^{-\Omega(n)}$ in their $\log m$ -bit encryption scheme with the security parameter n if the adversary has only $o\left(\frac{n \log n}{m \log m}\right)$ encryption keys.

2 Information-Theoretic Bounds

In this section, we present the general bounds for CSI and TCS. We first introduce basic notions and useful lemmas for our proofs in Section 2.1. We then give the general upper bounds for CSI and TCS in Section 2.2. We also prove the general lower bounds for the sample complexity of CSI and TCS in Section 2.3.

2.1 Basic Notions and Useful Lemmas

Any quantum operations for extracting classical information from quantum states can be generally described by the positive operator-valued measure (POVM) [35, 21]. A POVM $M = \{M_i\}_{i \in S}$ associated with a set of outcomes S is a set of Hermitian matrices satisfying that $M_i \geq 0$ ($i \in S$) and $\sum_{i \in S} M_i = I$. Then the probability of obtaining outcome $k \in S$ by the POVM M from a quantum state ρ is given by $\text{tr}(M_k \rho)$.

The trace norm of a matrix $X \in \mathbb{C}^{d \times d}$ is useful to estimate success probability of quantum state distinction for two states, and is defined as $\|X\|_{\text{tr}} = \max_{\|Y\| \leq 1} \langle Y, X \rangle = \text{tr} \sqrt{X^\dagger X}$, where $\|Y\|$ is the l_2 -norm of a matrix Y and

$\langle Y, X \rangle = \text{tr} Y^\dagger X$ is the matrix inner product. It is well known that for any two quantum states ρ_0 and ρ_1 the average success probability of the optimal POVM distinguishing between two quantum states is equal to $\frac{1}{2} + \frac{1}{4} \|\rho_0 - \rho_1\|_{\text{tr}}$, i.e., $\frac{1}{2} \max_{M=\{M_0, M_1\}} (\text{tr} M_0 \rho_0 + \text{tr} M_1 \rho_1) = \frac{1}{2} + \frac{1}{4} \|\rho_0 - \rho_1\|_{\text{tr}}$. See [4] for more details on the matrix analysis and [35, 21] on basics of the quantum information theory.

We make use of the PGM in order to prove the general upper bound for CSI. The following lemma shown by Hayashi and Nagaoka [22] is useful to estimate the error probability of the pretty good measurement. (See also Lemma 4.5 in [21].)

*Strictly speaking, our bound is better than theirs up to a constant factor.

Lemma 2.1 (Hayashi and Nagaoka [22]) For any Hermitian matrices S and T satisfying that $I \geq S \geq 0$ and $T \geq 0$, it holds that $I - \sqrt{S + T}^{-1} S \sqrt{S + T}^{-1} \leq 2(I - S) + 4T$, where $\sqrt{S + T}^{-1}$ is the generalized inverse matrix of $\sqrt{S + T}$.

In our several proofs, we need to calculate the rank of a coset state. The following lemma gives the estimation of the rank.

Lemma 2.2 For any coset state for a subgroup H of a finite group G , it holds that $\text{rank}(\rho_H) = \frac{|G|}{|H|}$.

Proof. Let $|\psi\rangle$ be a purification of ρ_H described as $|\psi\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle_A |f_H(g)\rangle_B$, where f_H is the given function in the definition of HSP. Tracing out the register A , we have $\text{rank}(\text{tr}_A |\psi\rangle\langle\psi|) = |G/H|$. Since $\text{rank}(\text{tr}_A |\psi\rangle\langle\psi|) = \text{rank}(\text{tr}_B |\psi\rangle\langle\psi|)$, we obtain $\text{rank}(\rho_H) = \frac{|G|}{|H|}$. \square

2.2 Lower Bounds

We next prove the key theorem on lower bounds for CSI by a simple information-theoretic argument. This theorem generally gives the necessary number of identical samples of an unknown coset state for the identification.

Theorem 2.3 Let \mathcal{H} be any set of candidate subgroups of a finite group G . Then, the sample complexity of CSI for \mathcal{H} is at least $\Omega\left(\frac{\log |\mathcal{H}|}{\log \max_{H \in \mathcal{H}} |H|}\right)$.

Proof. Let $M = \{M_H\}_{H \in \mathcal{H}}$ be any POVM associated with $S_{\mathcal{H}}$ using k samples of the coset state. By using the fact that $|\langle X, Y \rangle| \leq \|X\| \|Y\|_{\text{tr}}$ for any matrices $X, Y \in \mathbb{C}^{d \times d}$, the probability of M obtaining correct outcome is upper bounded by

$$\begin{aligned} \frac{1}{|\mathcal{H}|} \sum_{H \in \mathcal{H}} \text{tr} M_H \rho_H^{\otimes k} &= \frac{1}{|\mathcal{H}|} \sum_{H \in \mathcal{H}} \langle M_H, \rho_H^{\otimes k} \rangle \\ &\leq \frac{1}{|\mathcal{H}|} \sum_{H \in \mathcal{H}} \|\rho_H^{\otimes k}\| \|M_H\|_{\text{tr}} = \frac{1}{|\mathcal{H}|} \sum_{H \in \mathcal{H}} \|\rho_H^{\otimes k}\| \text{tr} \left(\sqrt{M_H^\dagger M_H} \right) = \frac{1}{|\mathcal{H}|} \sum_{H \in \mathcal{H}} \|\rho_H^{\otimes k}\| \text{tr} M_H \\ &\leq \frac{1}{|\mathcal{H}|} \max_{H \in \mathcal{H}} \|\rho_H\|^k \sum_{H \in \mathcal{H}} \text{tr} M_H = \frac{1}{|\mathcal{H}|} \max_{H \in \mathcal{H}} \|\rho_H\|^k \text{tr} \left(\sum_{H \in \mathcal{H}} M_H \right) = \frac{(\max_{H \in \mathcal{H}} \|\rho_H\| |G|)^k}{|\mathcal{H}|}. \end{aligned}$$

Thus, the success probability of any quantum algorithm that solves CSI with k coset states is upper bounded by $\frac{(\max_{H \in \mathcal{H}} \|\rho_H\| |G|)^k}{|\mathcal{H}|}$. Since the coset state $\rho_H = \frac{1}{|G/H|} \sum_{g \in G/H} |gH\rangle\langle gH|$ for any subgroup H is a uniform summation of the matrices $|gH\rangle\langle gH|$ orthogonal to each other, we obtain $\|\rho_H\| = 1/\text{rank}(\rho_H)$. It follows that $\|\rho_H\| = |H|/|G|$ by Lemma 2.2. The success probability is thus at most $\frac{(\max_{H \in \mathcal{H}} |H|)^k}{|\mathcal{H}|}$, which implies that any quantum algorithm that solves CSI for \mathcal{H} requires $\Omega\left(\frac{\log |\mathcal{H}|}{\log \max_{H \in \mathcal{H}} |H|}\right)$ coset states in order to attain constant success probability. \square

As mentioned in Section 1, we do not have to identify a hidden subgroup to solve TCS. Thus, we cannot expect the same technique as the proof of the lower bound for CSI to work for that of TCS. We give another proof technique to obtain the lower bound for TCS.

Theorem 2.4 Let \mathcal{H} be any set of candidate subgroups of a finite group G . The sample complexity of TCS for \mathcal{H} is at least $\Omega\left(\frac{\log |\mathcal{H}|}{\log(\max_{H \in \mathcal{H}} |H|)}\right)$ if $|H|$ is a prime for every $H \in \mathcal{H}$.

Proof. We first show that the success probability of solving TCS for \mathcal{H} is upper bounded by that of identification for certain two quantum states. Let $M = \{M_0, M_1\}$ be any POVM associated with $\{|id\rangle, \mathcal{H}\}$. The success probability of M is given by $\min\{\text{tr} M_0 (I/|G|)^{\otimes k}, \min_{\rho_H \in S_{\mathcal{H}}} \{\text{tr} M_1 \rho_H^{\otimes k}\}\}$. Also, it holds by the linearity of the trace and the POVM that $\text{tr} M_1 \left(\frac{1}{|\mathcal{H}|} \sum_{\rho_H \in S_{\mathcal{H}}} \rho_H^{\otimes k} \right) = \frac{1}{|\mathcal{H}|} \sum_{\rho_H \in S_{\mathcal{H}}} \text{tr} M_1 \rho_H^{\otimes k} \geq \min_{\rho_H \in S_{\mathcal{H}}} \text{tr} M_1 \rho_H^{\otimes k}$. Thus, the success probability is at most $\min\{\text{tr} M_0 (I/|G|)^{\otimes k}, \frac{1}{|\mathcal{H}|} \sum_{\rho_H \in S_{\mathcal{H}}} \text{tr} M_1 \rho_H^{\otimes k}\}$. This is equal to the success probability of the identification for $(I/|G|)^{\otimes k}$ and $\frac{1}{|\mathcal{H}|} \sum_{\rho_H \in S_{\mathcal{H}}} \rho_H^{\otimes k}$.

Note that we cannot apply the argument of Theorem 2.3 to the identification. Instead, we directly evaluate an upper bound of the trace norm of the matrix $X = \frac{1}{|\mathcal{H}|} \sum_{\rho_H \in S_{\mathcal{H}}} \rho_H^{\otimes k} - (I/|G|)^{\otimes k}$. Then the success probability of the identification is at most $\frac{1}{2} + \frac{1}{4}\|X\|_{\text{tr}}$ by the property of the trace norm. Naïvely expanding X , we obtain by the triangle inequality

$$\begin{aligned}
\|X\|_{\text{tr}} &= \left\| \frac{1}{|\mathcal{H}|} \sum_{H \in \mathcal{H}} \frac{1}{|G|^k} \sum_{g_1, \dots, g_k \in G} \left(\sum_{h_1, \dots, h_k \in H} |g_1, \dots, g_k\rangle \langle g_1 h_1, \dots, g_k h_k| - |g_1, \dots, g_k\rangle \langle g_1, \dots, g_k| \right) \right\|_{\text{tr}} \\
&= \left\| \frac{1}{|\mathcal{H}|} \frac{1}{|G|^k} \sum_{g_1, \dots, g_k \in G} \left(\sum_{H \in \mathcal{H}} \sum_{\substack{h_1, \dots, h_k \in H \\ (h_1, \dots, h_k) \neq (id, \dots, id)}} |g_1, \dots, g_k\rangle \langle g_1 h_1, \dots, g_k h_k| \right) \right\|_{\text{tr}} \\
&\leq \frac{1}{|\mathcal{H}| |G|^k} \sum_{g_1, \dots, g_k \in G} \left\| \sum_{H \in \mathcal{H}} \sum_{\substack{h_1, \dots, h_k \in H \\ (h_1, \dots, h_k) \neq (id, \dots, id)}} \langle g_1 h_1, \dots, g_k h_k| \right\| \\
&= \frac{1}{|\mathcal{H}|} \sqrt{\left(\sum_{H, H' \in \mathcal{H}} |H \cap H'|^k \right) - |\mathcal{H}|^2} = \sqrt{\frac{1}{|\mathcal{H}|^2} \left(\sum_{H \in \mathcal{H}} |H|^k + \sum_{H \neq H'} |H \cap H'|^k \right) - 1} \\
&\leq \sqrt{\frac{\max_{H \in \mathcal{H}} |H|^k}{|\mathcal{H}|}}.
\end{aligned}$$

In the last inequality, we use the fact that $|H \cap H'| = 1$ for any distinct H and H' , which follows from the prime order of the subgroups.

In order to have this trace norm larger than some positive constant, k must be $\Omega\left(\frac{\log |\mathcal{H}|}{\log(\max_{H \in \mathcal{H}} |H|)}\right)$. Thus $\Omega\left(\frac{\log |\mathcal{H}|}{\log(\max_{H \in \mathcal{H}} |H|)}\right)$ samples are necessary for constant advantage. \square

2.3 Upper Bounds

We present general upper bounds for CSI and TCS in this section. First, we prove the upper bound for CSI by using the PGM for $S_{\mathcal{H}}$. In this proof, we make use of Lemma 2.1 to estimate the error probability of the PGM.

Theorem 2.5 Let \mathcal{H} be any set of candidate subgroups of a finite group G . Then, the sample complexity of CSI for \mathcal{H} is at most $O\left(\frac{\log |\mathcal{H}|}{\log \min_{H \neq H' \in \mathcal{H}} (|H|/|H \cap H'|)}\right)$.

Proof. Let P_H be the projection onto the space spanned by $\text{supp}(\rho_H)$ for $H \in \mathcal{H}$. We consider the pretty good measurement $M = \{\Sigma^{-1/2} P_H \Sigma^{-1/2}\}_{H \in \mathcal{H}}$ for $S_{\mathcal{H}}$, where $\Sigma = \sum_{H \in \mathcal{H}} P_H$. Let $\gamma_{H, H'} = |\{(h, h') \in H \times H' : hh' = id\}| = |H \cap H'|$ for $H, H' \in \mathcal{H}$. We now prove that the error probability of M is at most $4 \sum_{H' \neq H} \frac{(\gamma_{H, H'})^k}{|H'|^k}$ if the given state is ρ_H .

Since we have

$$\text{tr} \rho_H \rho_{H'} = \frac{1}{|G|^2} \sum_{g, g' \in G} \sum_{h \in H, h' \in H'} \text{tr} |g\rangle \langle gh| |g'\rangle \langle g'h'| = \frac{1}{|G|^2} \sum_{g \in G} \sum_{h \in H, h' \in H'} \text{tr} |g\rangle \langle gh h'| = \frac{1}{|G|^2} \sum_{g \in G} \sum_{\substack{h \in H, h' \in H' \\ hh' = id}} 1 = \frac{\gamma_{H, H'}}{|G|},$$

it follows that $\text{tr} P_H \rho_{H'} = \frac{\gamma_{H, H'}}{|G|} \frac{|G|}{|H'|} = \frac{\gamma_{H, H'}}{|H'|}$. Setting $S = P_H^{\otimes k}$ and $T = \sum_{H' \neq H} P_{H'}^{\otimes k}$ in Lemma 2.1, if the given state is ρ_H , the error probability of M is

$$\text{tr}(I - \Sigma^{-1/2} P_H^{\otimes k} \Sigma^{-1/2}) \rho_H^{\otimes k} \leq 2 \text{tr}(I - P_H^{\otimes k}) \rho_H^{\otimes k} + 4 \text{tr} \left(\sum_{H' \neq H} P_{H'}^{\otimes k} \right) \rho_H^{\otimes k} = 4 \sum_{H' \neq H} (\text{tr} P_{H'} \rho_H)^k = 4 \sum_{H' \neq H} \frac{(\gamma_{H, H'})^k}{|H'|^k}.$$

We can easily obtain the upper bound of the error probability from the above estimation. Since we have

$$4 \max_{H \in \mathcal{H}} \sum_{H' \neq H} \frac{(\gamma_{H,H'})^k}{|H'|^k} \leq 4|\mathcal{H}| \max_{H \neq H' \in \mathcal{H}} \left(\frac{|H \cap H'|}{|H|} \right)^k,$$

the error probability of M is at most $4|\mathcal{H}| \max_{H \neq H' \in \mathcal{H}} \left(\frac{|H \cap H'|}{|H|} \right)^k$, which implies that $O\left(\frac{\log |\mathcal{H}|}{\log \min_{H \neq H' \in \mathcal{H}} (|H|/|H \cap H'|)}\right)$ samples of coset states are sufficient for constant success probability. \square

Next, we present the general upper bound for TCS as follows. This upper bound can be attained by a simple two-valued POVM.

Theorem 2.6 Let \mathcal{H} be any set of candidate subgroups of a finite group G . Then the sample complexity of TCS for \mathcal{H} is at most $O\left(\frac{\log |\mathcal{H}|}{\log \min_{H \in \mathcal{H}} |H|}\right)$.

Proof. We consider a projection T onto the space spanned by $\bigcup_{H \in \mathcal{H}} \text{supp}(\rho_H^{\otimes k})$. It obviously holds that $\text{tr} T \rho_H^{\otimes k} = 1$ for every $H \in \mathcal{H}$. On the other hand, the error probability is given by $\text{tr} T(I/|G|)^{\otimes k}$. Then we have $\text{tr} T(I/|G|)^{\otimes k} = \frac{\text{rank}(T)}{|G|^k} \leq \frac{\sum_{H \in \mathcal{H}} \text{rank}(\rho_H)^k}{|G|^k}$. Since $\text{rank}(\rho_H) = |G|/|H|$ by Lemma 2.2, we obtain $\frac{\sum_{H \in \mathcal{H}} \text{rank}(\rho_H)^k}{|G|^k} = \frac{\sum_{H \in \mathcal{H}} (|G|/|H|)^k}{|G|^k} \leq \frac{|\mathcal{H}|}{\min_{H \in \mathcal{H}} |H|^k}$. This implies that at most $O\left(\frac{\log |\mathcal{H}|}{\log \min_{H \in \mathcal{H}} |H|}\right)$ samples of coset states are sufficient for constant advantage. \square

3 Security Evaluation of Quantum Encryption Schemes

Our arguments are applicable not only to bounds for HSP but also to security evaluation of quantum cryptographic schemes. In this section, we apply our arguments to evaluation of the information-theoretic security of the quantum encryption schemes proposed in [25, 26]. As mentioned in Section 1, they proposed single-bit and multi-bit quantum encryption schemes. While they gave the complexity-theoretic security to the single-bit scheme under the assumption of the worst-case hardness of the decisional graph automorphism problem, the multi-bit one has no security proof. Also, they have already proven in [26] that any computationally unbounded quantum algorithm cannot solve a certain quantum state distinction problem that underlies the single-bit scheme with few samples by reducing the solvability of their distinction problem to the result of [17]. On the other hand, the security of their encryption schemes, as well as the underlying problem for their multi-bit scheme, are not evaluated yet from a viewpoint of the quantum information theory.

Their schemes make use of certain quantum states for their encryption keys and ciphertexts. We now call these quantum states *encryption-key states* and *cipherstates*, respectively. Since their multi-bit encryption scheme contains the single-bit one as a special case if we ignore its efficiency and complexity-theoretic security, we only discuss their multi-bit scheme in this paper.

We now describe their multi-bit encryption scheme in detail. Assume that the message length parameter m divides the security parameter n , where $m \in \{2, \dots, n\}$. Let $\mathcal{K}_n^m = \{h : h = (a_1 \cdots a_m) \cdots (a_{n-m+1} \cdots a_n), a_i \in \{1, \dots, n\}, a_i \neq a_j (i \neq j)\} \subset S_n$, i.e., a set of the permutations composed of n/m disjoint cyclic permutations, which is used for the decryption key. In this scheme, we exploit the following quantum state for a message s : $\rho_h^{(s)} = \frac{1}{mn!} \sum_{g \in S_n} \left(\sum_{k=0}^{m-1} \omega_m^{ks} |gh^k\rangle \right) \left(\sum_{l=0}^{m-1} \omega_m^{-ls} \langle gh^l| \right)$, where $\omega_m = e^{2\pi i/m}$ and $h \in \mathcal{K}_n^m$. Note that $\rho_h^{(0)}$ is the coset state for the hidden subgroup $\{id, h, \dots, h^{m-1}\}$.

We now refer to as (n, m) -QES their multi-bit encryption scheme with the security parameter n and the message length parameter m . The protocol of (n, m) -QES is summarized as follows.

Protocol: (n, m) -QES

- (1) The receiver Bob chooses his decryption key h uniformly at random from \mathcal{K}_n^m and generates the encryption-key states $\sigma_h = (\rho_h^{(0)}, \dots, \rho_h^{(m-1)})$.
- (2) The sender Alice requests the encryption-key state σ_h to Bob. She picks $\rho_h^{(s)}$ up from σ_h as the cipherstate corresponding to her classical message $s \in \{0, \dots, m-1\}$ and then sends it to him.

(3) Bob decrypts her cipherstate $\rho_h^{(s)}$ with his decryption key h .

We assume the same adversary model except for Eve's computational power as the original ones in [25, 26]. Note that the eavesdropper Eve can also request the same encryption-key states to Bob as one of senders. Eve in advance requests the encryption-key states to Bob. When Alice sends to Bob her cipherstate that Eve wants to eavesdrop, Eve picks up Alice's cipherstate and then tries to extract Alice's message from the cipherstate with the encryption-key states by computationally unbounded quantum computer, i.e., Eve can apply an arbitrary POVM over the cipherstates and encryption-key states to extract Alice's message.

We consider a stronger security notion such that Eve cannot distinguish between even two candidates, i.e., she cannot find a non-negligible gap between $\text{tr} M_1(\rho_h^{(s)} \otimes \sigma_h^{\otimes k})$ and $\text{tr} M_1(\rho_h^{(s')} \otimes \sigma_h^{\otimes k})$ even by the optimal POVM $M = \{M_0, M_1\}$ when Bob chooses h uniformly at random. This notion naturally extends the computational indistinguishability of encryptions, which is the standard security notion in the modern cryptography [13], to the information-theoretic one.

Since the gap is at most $\frac{1}{2} \left\| \frac{1}{|\mathcal{K}_n^m|} \sum_{h \in \mathcal{K}_n^m} \rho_h^{(s)} \otimes \sigma_h^{\otimes k} - \rho_h^{(s')} \otimes \sigma_h^{\otimes k} \right\|_{\text{tr}}$, this notion can be formalized by the trace norm between them. Then, we say that the cipherstates are *information-theoretically indistinguishable within k encryption-key states* if $\left\| \frac{1}{|\mathcal{K}_n^m|} \sum_{h \in \mathcal{K}_n^m} \rho_h^{(s)} \otimes \sigma_h^{\otimes k} - \rho_h^{(s')} \otimes \sigma_h^{\otimes k} \right\|_{\text{tr}} = 2^{-\Omega(n)}$.

For this security notion, we can obtain the following theorem by our information-theoretic arguments. The proof is almost straightforward by Theorem 2.4.

Theorem 3.1 The cipherstates of (n, m) -QES are information-theoretically indistinguishable within $o\left(\frac{n \log n}{m \log m}\right)$ encryption-key states.

Proof. Let $l_s = \left\| \frac{1}{|\mathcal{K}_n^m|} \sum_{h \in \mathcal{K}_n^m} \rho_h^{(s)} \otimes \sigma_h^{\otimes k} - (I/n!)^{\otimes mk+1} \right\|_{\text{tr}}$. Then the trace norm between two state sequences given in the definition of the information-theoretic indistinguishability is at most $l_s + l_{s'}$ by the triangle inequality. Since the trace norm is invariant under unitary transformations, we can show that $l_s + l_{s'} = 2l_0$ by taking appropriate unitary operators. Then we can prove that $l_0 \leq \sqrt{m^{mk+1}/|\mathcal{K}_n^m|}$ by the argument of Theorem 2.4. Since we have $|\mathcal{K}_n^m| \approx \frac{m^{1/2} n^{n-n/m}}{e^{n-n/m}}$ by the standard counting method and the Stirling approximation, the trace norm is at most $2^{-\Omega(n)}$ if $k = o\left(\frac{n \log n}{m \log m}\right)$. \square

For example, when we set $m = n^\varepsilon$ for any constant $0 < \varepsilon < 1$, we obtain the $\varepsilon \log n$ -bit encryption scheme whose cipherstates are information-theoretically indistinguishable within $o(n^{1-\varepsilon})$ encryption-key states.

4 Concluding Remarks

In this paper, we have shown general bounds for CSI and TCS, and an application to the security evaluation of the quantum encryption schemes. We believe such an information-theoretic approach will help constructions of efficient quantum algorithms for non-Abelian HSPs as in the case of [2]. After our preliminary version of this paper, Harrow and Winter followed our approach to prove the existence of a quantum measurement for identifying general quantum states and lower bounds of samples for the identification [19]. Their results generalize and improve our bounds for CSI.

Acknowledgements. The authors would like to thank François Le Gall, Cristopher Moore, Christopher Portmann and Tomoyuki Yamakami for helpful discussions and comments. MH is grateful to Hiroshi Imai with the ERATO-SORST QCI project for support. AK was supported by the Ministry of Education, Science, Sports and Culture, Grant-in-Aid for Young Scientists (B) No.17700007, 2005 and for Scientific Research on Priority Areas No.16092206.

References

- [1] Gorjan Alagic, Cristopher Moore, and Alexander Russell. Strong Fourier sampling fails over G^n . quant-ph/0511054, 2005.

- [2] Dave Bacon, Andrew M. Childs, and Wim van Dam. From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups. In *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science*, pages 469–478, 2005.
- [3] Robert Beals. Quantum computation of fourier transforms over symmetric groups. In *Proceedings of the 29th annual ACM Symposium on Theory of Computing*, pages 48–53, 1997.
- [4] Rajendra Bhatia. *Matrix Analysis*. Springer, 1997.
- [5] Dan Boneh and Richard J. Lipton. Quantum cryptanalysis of hidden linear functions (extended abstract). In *Advances in Cryptology - CRYPTO '95*, LNCS 963, pages 424–437. Springer, 1995.
- [6] Gilles Brassard and Peter Høyer. An exact quantum polynomial-time algorithm for Simon’s problem. In *Proceedings of the 5th Israel Symposium on Theory of Computing and Systems*, pages 12–23, 1997.
- [7] Gilles Brassard, Peter Høyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. *Quantum Computation and Information*, 305:53–74, 2002.
- [8] Mark Ettinger and Peter Høyer. A quantum observable for the graph isomorphism problem. quant-ph/9901029, 1999.
- [9] Mark Ettinger and Peter Høyer. On quantum algorithms for noncommutative hidden subgroups. *Advances in Applied Mathematics*, 25:239–251, 2000.
- [10] Mark Ettinger, Peter Høyer, and Emanuel Knill. The quantum query complexity of the hidden subgroup problem is polynomial. *Information Processing Letter*, 91:43–48, 2004.
- [11] Katalin Friedl, Gábor Ivanyos, Frédéric Magniez, Miklos Santha, and Pranab Sen. Hidden translation and orbit coset in quantum computing. In *Proceedings of the 35th Annual ACM Symposium on Theory of Computing*, pages 1–9, 2003.
- [12] Dmitry Gavinsky. Quantum solution to the hidden subgroup problem for poly-near-hamiltonian groups. *Quantum Information and Computation*, 4:229–235, 2004.
- [13] Oded Goldreich. *Foundations of Cryptography: Basic Tools*. Cambridge University Press, 2001.
- [14] Michelangelo Grigni, Leonard J. Schulman, Monica Vazirani, and Umesh Vazirani. Quantum mechanical algorithms for the nonabelian hidden subgroup problem. *Combinatorica*, 24(1):137–154, 2004.
- [15] Sean Hallgren. Polynomial-time quantum algorithms for Pell’s equation and the principal ideal problem. In *Proceedings of the 34th Annual ACM Symposium on Theory of Computing*, pages 653–658, 2002.
- [16] Sean Hallgren. Fast quantum algorithms for computing the unit group and class group of a number field. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, pages 468–474, 2005.
- [17] Sean Hallgren, Cristopher Moore, Martin Rötteler, Alexander Russell, and Pranab Sen. Limitations of quantum coset states for graph isomorphism. In *Proceedings of the 38th ACM Symposium on Theory of Computing*, pages 604–617, 2006.
- [18] Sean Hallgren, Alexander Russell, and Amnon Ta-Shma. The hidden subgroup problem and quantum computation using group representations. *SIAM Journal on Computing*, 32(4):916–934, 2003.
- [19] Aram W. Harrow and Andreas Winter. How many copies are needed for state discrimination? quant-ph/0606131, 2006.
- [20] Paul Hausladen and William K. Wootters. A ‘pretty good’ measurement for distinguishing quantum states. *Journal of Modern Optics*, 41:2385–2390, 1994.

- [21] Masahito Hayashi. *Quantum Information Theory: An Introduction*. Springer, 2006.
- [22] Masahito Hayashi and Hiroshi Nagaoka. General formulas for capacity of classical-quantum channels. *IEEE Transactions on Information Theory*, 49:1753–1768, 2002.
- [23] Yoshifumi Inui and François Le Gall. An efficient algorithm for the hidden subgroup problem over a class of semi-direct product groups. In *Proceedings of the 4th ERATO Conference on Quantum Information Science*, 2004. See also <http://jp.arxiv.org/abs/quant-ph/0412033>.
- [24] Gábor Ivanyos, Frédéric Magniez, and Miklos Santha. Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem. *International Journal of Foundations of Computer Science*, 14(5):723–740, 2003.
- [25] Akinori Kawachi, Takeshi Koshihara, Harumichi Nishimura, and Tomoyuki Yamakami. Computational indistinguishability between quantum states and its cryptographic application. In *Advances in Cryptology - EUROCRYPT '05*, LNCS 3494, pages 268–284. Springer, 2005.
- [26] Akinori Kawachi, Takeshi Koshihara, Harumichi Nishimura, and Tomoyuki Yamakami. Computational indistinguishability between quantum states and its cryptographic application. Full version of [25]. Available at quant-ph/0403069, 2006.
- [27] Julia Kempe and Aner Shalev. The hidden subgroup problem and permutation group theory. In *Proceedings of the 16th ACM-SIAM Symposium on Discrete Algorithms*, pages 1118–1125, 2005.
- [28] Alexei Kitaev. Quantum measurements and the abelian stabilizer problem. quant-ph/9511026, 1995.
- [29] Johannes Köbler, Uwe Schöning, and Jacobo Torán. *The Graph Isomorphism Problem: Its Structural Complexity*. Birkhäuser Boston Inc., 1993.
- [30] Cristopher Moore, Daniel Rockmore, Alexander Russell, and Leonard J. Schulman. The hidden subgroup problem in affine groups: basis selection in Fourier sampling. In *Proceedings of the 15th ACM-SIAM Symposium on Discrete Algorithms*, pages 1106–1115, 2004.
- [31] Cristopher Moore and Alexander Russell. For distinguishing conjugate hidden subgroups, the pretty good measurement is as good as it gets. quant-ph/0501177, 2005.
- [32] Cristopher Moore and Alexander Russell. The symmetric group defies strong Fourier sampling: Part II. quant-ph/0501066, 2005.
- [33] Cristopher Moore, Alexander Russell, and Leonard J. Schulman. The symmetric group defies strong Fourier sampling. In *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science*, pages 479–488, 2005. See also quant-ph/0501056 and quant-ph/0501066.
- [34] Michele Mosca and Artur Ekert. The hidden subgroup problem and eigenvalue estimation on a quantum computer. In *Proceedings of the 1st NASA International Conference on Quantum Computing and Quantum Communication*, LNCS 1501, pages 174–188. Springer, 1999.
- [35] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [36] Oded Regev. Quantum computation and lattice problems. *SIAM Journal on Computing*, 33(3):738–760, 2004.
- [37] Martin Rötteler and Thomas Beth. Polynomial-time solution to the hidden subgroup problem for a class of non-abelian groups. quant-ph/9812070, 1998.

- [38] Arthur Schmidt and Ulrich Vollmer. Polynomial time quantum algorithm for the computation of the unit group of a number field. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, pages 475–480, 2005.
- [39] Pranab Sen. Random measurement bases, quantum state distinction and applications to the hidden subgroup problem. In *Proceedings of the 21st Annual IEEE Conference on Computational Complexity*, 2006.
- [40] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.
- [41] Daniel R. Simon. On the power of quantum computation. *SIAM Journal on Computing*, 26(5):1474–1483, 1997.